GameOver Zeus (GOZ) Malware and Botnet Architecture

BUILDING THE BOTNET

Cyber criminals create a network of compromised computers by sending emails with embedded malicious links or attachments or by enticing users to visit infected websites. Once infected, covertly installed malware connects computers to the botnet infrastructure without the owners' knowledge.

COMMAND AND CONTROL SERVERS

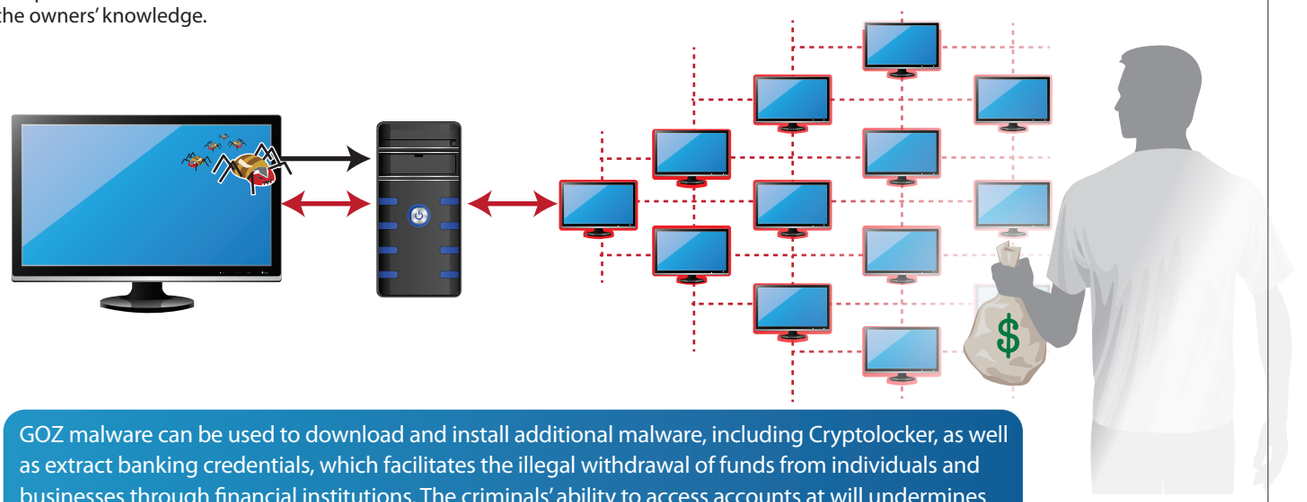
At the core of the botnet are servers which issue commands orchestrating various criminal activities.

BOTNET USE

Infected computers are organized together to implement illicit orders from the command and control servers.

A QUIET THREAT

Botnets typically operate without obvious visible evidence and can remain operational for years.

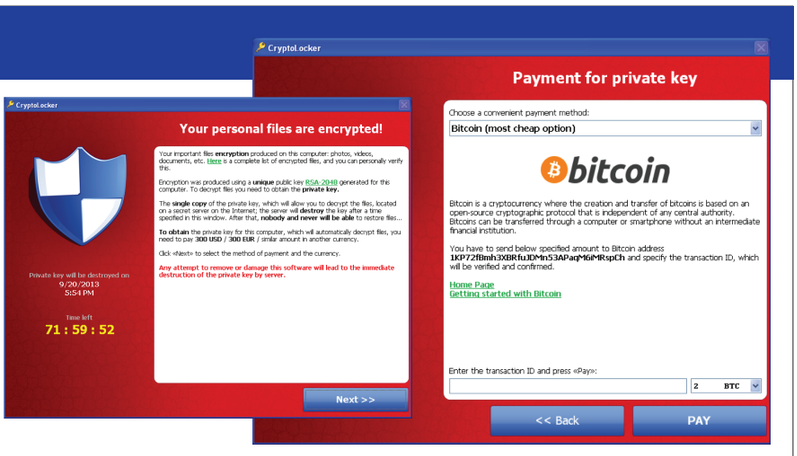


GOZ malware can be used to download and install additional malware, including Cryptolocker, as well as extract banking credentials, which facilitates the illegal withdrawal of funds from individuals and businesses through financial institutions. The criminals' ability to access accounts at will undermines business integrity and public confidence and has the potential to threaten financial infrastructure.

CryptoLocker Malware

Computers compromised by the GOZ botnet may also be infected with CryptoLocker, a form of "ransomware."

- Victim files are encrypted and held "hostage" until the victim makes payment
- More than 121,000 victims in the United States and 234,000 victims worldwide
- There were approximately $30 million in ransom payments between September and December 2013



GOZ/CryptoLocker Scope

- **More than 1 million GOZ infections globally**
- **Roughly 25% of infected computers are located in the United States**
- **Losses estimated globally in the hundreds of millions of dollars**
- **Key participation of 10 partner countries in support of takedown operation**